CLAIMS

What is claimed is:

1. A method for performing ephemeral decryption comprising:

associating an expiration time with at least an ephemeral decryption key of an ephemeral key pair comprising said ephemeral decryption key and an ephemeral encryption key;

storing at least said ephemeral decryption key in a memory within a tamper resistant cryptographic processor unit such that said ephemeral decryption key is not accessible external of said tamper resistant cryptographic processor unit;

receiving at said tamper resistant cryptographic processor unit from a first node an ephemeral message encrypted with said ephemeral encryption key; and

decrypting said ephemeral message within said tamper resistant cryptographic processor unit using said ephemeral decryption key to form a decrypted ephemeral message in the event said ephemeral message is associated with a message time that is prior to said expiration time.

2. The method of claim 1 further including the step of forwarding said decrypted ephemeral message to said first node.

ATTORNEY DOCKET NO. P5529
WEINGARTEN, SCHURGIN,
GAGNEBIN & HAYES LLP
TEL. (617) 542-2290
FAX. (617) 451-0313

3. The method of claim 1 further including the step of forwarding said decrypted ephemeral message to a second node.

4. The method of claim 1 further including the step of generating said ephemeral key pair within said tamper resistant cryptographic processor unit.

5. The method of claim 1 further including the step of extinguishing at least said ephemeral decryption key following the associated expiration time to prevent said ephemeral message from becoming accessible subsequent to said expiration time.

6. The method of claim 5 wherein said extinguishing step comprises the step of erasing said ephemeral decryption key.

7. The method of claim 5 wherein said extinguishing step comprises the step of preventing messages that are decrypted using said ephemeral decryption key from being forwarded outside of said tamper resistant cryptographic processor unit.

8. The method of claim 5 wherein said extinguishing step comprises the step of preventing messages that are encrypted using said encryption key from being decrypted using said ephemeral decryption key.

9. The method of claim 1 further including the step of

ATTORNEY DOCKET NO. P5529
WEINGARTEN, SCHURGIN,
GAGNEBIN & HAYES LLP
TEL. (617) 542-2290
FAX. (617) 451-0313

erasing said ephemeral decryption key within said tamper resistant cryptographic processor unit in the event said message time is subsequent to said expiration time.

10. The method of claim 1 wherein said tamper resistant cryptographic processor unit includes an internal clock operative to generate said message time and said method includes the step of erasing said ephemeral decryption key in response to a determination that said message time is subsequent to said expiration time.

11. The method of claim 1 wherein said message time corresponds to a timestamp accompanying said received ephemeral message.

12. The method of claim 1 wherein said message time corresponds to a timestamp generated by a clock within said tamper resistant cryptographic processor unit.

13. The method of claim 1 wherein said message time corresponds to a time received from a trusted time authority.

14. The method of claim 13 further including the steps of:

in response to receipt of said ephemeral message at said tamper resistant cryptographic processor unit, forwarding a request to said trusted time authority for said message time;

receiving a time message including said message time from said trusted time authority; and

associating said message time with said ephemeral message.

15. The method of claim 14 further including the steps of:

signing by said trusted time authority said time message; and

verifying said signed time message.

16. The method of claim 1 further including the step of erasing at least said ephemeral decryption key upon detection within said tamper resistant cryptographic processor unit of a predetermined condition indicative of an attempt to access at least said ephemeral decryption key.

17. The method of claim 1 wherein said first node is coupled to a global communications network.

18. The method of claim 1 wherein said first node is coupled to a local area network.

19. A method for communicating an ephemeral message comprising:

associating an expiration time with at least an ephemeral decryption key of an ephemeral key pair including said ephemeral decryption key and an ephemeral encryption key;

ATTORNEY DOCKET NO. P5529
WEINGARTEN, SCHURGIN,
GAGNEBIN & HAYES LLP
TEL. (617) 542-2290
FAX. (617) 451-0313

storing at least said ephemeral decryption key in a memory within a tamper resistant cryptographic processor unit in communication with a first node such that said ephemeral decryption key is not accessible external of said tamper resistant processor unit;

encrypting at a second node a message to form an encrypted ephemeral message, wherein said encrypting is performed using said ephemeral encryption key;

in a first transmitting step, transmitting said ephemeral message to a third node;

forwarding by said third node to said tamper resistant cryptographic processor unit via said first node said encrypted ephemeral message;

decrypting said encrypted ephemeral message within said tamper resistant cryptographic processor unit using said ephemeral decryption key in the event said message is associated with a message time prior to said expiration time;

forwarding said decrypted ephemeral message from said tamper resistant cryptographic processor cryptographic processor unit to a fourth node; and

in a second transmitting step, transmitting said decrypted ephemeral message from said fourth node to said third node.

20. The method of claim 19 wherein said first node and said fourth node are the same node.

ATTORNEY DOCKET NO. P5529
WEINGARTEN, SCHURGIN,
GAGNEBIN & HAYES LLP
TEL. (617) 542-2290
FAX. (617) 451-0313

21. The method of claim 19 further including the step of generating said ephemeral key pair within said tamper resistant cryptographic processor unit.

22. The method of claim 19 wherein said encrypting step includes the steps of encrypting said message at said second node with a third node encryption key having a corresponding third node decryption key held by said third node and encrypting said message encrypted using said third node encryption key using said ephemeral encryption key to form said encrypted ephemeral message; and

following said second transmitting step, decrypting said decrypted ephemeral message using said third node decryption key to reproduce said message.

23. An apparatus for use in ephemeral communications comprising:

a tamper resistant cryptographic processor unit including a memory, said unit operative to:

associate an expiration time with at least an ephemeral decryption key of an ephemeral key pair including an ephemeral encryption key and said ephemeral decryption key;

store at least said ephemeral decryption key in said memory such that said ephemeral decryption key is not accessible external of said tamper resistant cryptographic processor unit;

receive from a first node coupled to a network at said tamper resistant cryptographic processor

unit an ephemeral message that has been encrypted with said ephemeral encryption key;

decrypt said encrypted ephemeral message within said tamper resistant cryptographic processor unit using said ephemeral decryption key in the event said message is associated with a message time related to the time of receipt of said encrypted ephemeral message prior to said expiration time; and

forward said decrypted message to a second node.

24. The apparatus of claim 23 wherein said first node and said second node are the same node.

25. The apparatus of claim 23 wherein said tamper resistant cryptographic processor unit is operative to generate said ephemeral key pair including said ephemeral encryption key and said corresponding ephemeral decryption key within said tamper resistant cryptographic processor unit.

26. The apparatus of claim 23 wherein said tamper resistant cryptographic processor unit is further operative to extinguish said ephemeral decryption key in response to a determination that said message time is subsequent to said expiration time.

27. The apparatus of claim 26 wherein said tamper resistant cryptographic processor unit is operative to erase said ephemeral decryption key in response to a

ATTORNEY DOCKET NO. P5529
WEINGARTEN, SCHURGIN,
GAGNEBIN & HAYES LLP
TEL. (617) 542-2290
FAX. (617) 451-0313

determination that said message time is subsequent to said expiration time.

28. The apparatus of claim 26 wherein said tamper resistant cryptographic processor unit is operative to prevent decrypted ephemeral messages from being forwarded to the second node in response to said determination that said message time is subsequent to said expiration time.

29. The apparatus of claim 26 wherein said tamper resistant cryptographic processor unit is operative to prevent said encrypted ephemeral message from being decrypted using said ephemeral decryption key in response to a determination that said message time is subsequent to said expiration time.

30. The apparatus of claim 23 wherein said tamper resistant cryptographic processor unit is operative to erase said ephemeral decryption key within said tamper resistant processor unit in the event said received ephemeral message includes a timestamp that is subsequent to said expiration time.

31. The apparatus of claim 23 wherein said tamper resistant cryptographic processor unit further includes an internal clock and said tamper resistant cryptographic processor unit is operative to erase said ephemeral decryption key within said tamper resistant cryptographic processor unit in response to a determination that a clock time generated by said internal clock in response

ATTORNEY DOCKET NO. P5529
WEINGARTEN, SCHURGIN,
GAGNEBIN & HAYES LLP
TEL. (617) 542-2290
FAX. (617) 451-0313

to receipt of said ephemeral message is subsequent to said expiration time.

32. The apparatus of claim 23 wherein said tamper resistant cryptographic processor unit is operative to retrieve said message time from a trusted time authority and said tamper resistant cryptographic processor unit is operative to erase said ephemeral decryption key in the event said message time is subsequent to said expiration time.

33. The apparatus of claim 23 wherein said tamper resistant cryptographic processor unit is operative to erase at least said ephemeral decryption key in response to detection of a predetermined condition indicative of an attempt to access information within said tamper resistant cryptographic processor unit.

34. The apparatus of claim 23 wherein said tamper resistant cryptographic processor unit is operative to erase said ephemeral decryption key in response to detection of a predetermined condition indicative of an attempt to access said ephemeral decryption key.

35. A computer program product including a computer readable medium, said computer readable medium having a computer program stored thereon for use in ephemeral communication, said computer program being executable on a processor and comprising:

ATTORNEY DOCKET NO. P5529
WEINGARTEN, SCHURGIN,
GAGNEBIN & HAYES LLP
TEL. (617) 542-2290
FAX. (617) 451-0313

program code for associating an expiration time with at least an ephemeral decryption key of an ephemeral key pair including said ephemeral decryption key and a corresponding ephemeral encryption key;

program code for storing at least said ephemeral decryption key in a memory within a tamper resistant cryptographic processor unit such that said ephemeral decryption key is not accessible external of said tamper resistant cryptographic processor unit;

program code for receiving at said tamper resistant cryptographic processor unit from a first node an ephemeral message encrypted with said ephemeral encryption key; and

program code for decrypting said ephemeral message within said tamper resistant cryptographic processor unit using said ephemeral decryption key to form a decrypted ephemeral message in the event said message is associated with a message time prior to said expiration time.

36. The computer program product of claim 35 wherein said computer program further includes program code for forwarding said decrypted ephemeral message to said first node.

37. The computer program product of claim 35 wherein said computer program further includes program code for forwarding said decrypted ephemeral message to a second node.

ATTORNEY DOCKET NO. P5529
WEINGARTEN, SCHURGIN,
GAGNEBIN & HAYES LLP
TEL. (617) 542-2290
FAX. (617) 451-0313

38. A computer data signal, said computer data signal including a computer program for use in ephemeral communication, said computer program comprising:

program code for associating an expiration time with at least an ephemeral decryption key of an ephemeral key pair including said ephemeral decryption key and an ephemeral encryption key;

program code for storing at least said ephemeral decryption key in a memory within a tamper resistant cryptographic processor unit such that said ephemeral decryption key is inaccessible external of said tamper resistant cryptographic processor unit;

program code for receiving at said tamper resistant cryptographic processor unit from a first node an ephemeral message encrypted with said ephemeral encryption key; and

program code for decrypting said ephemeral message within said tamper resistant cryptographic processor unit using said ephemeral decryption key to form a decrypted ephemeral message in the event said message is associated with a message time prior to said expiration time.

39. The computer data signal of claim 38 wherein said computer program further includes program code for forwarding said decrypted ephemeral message to said first node.

40. The computer data signal of claim 38 wherein said computer program further includes program code for

forwarding said decrypted ephemeral message to a second node.

41. An apparatus for use in ephemeral communication of information comprising:

means for associating an expiration time with at least an ephemeral decryption key of an ephemeral key pair including said ephemeral decryption key and a corresponding ephemeral encryption key;

means for storing at least said ephemeral decryption key in a memory within said tamper resistant cryptographic processor unit such that said ephemeral decryption key is not accessible external of said tamper resistant cryptographic processor unit;

means for receiving at said tamper resistant cryptographic processor unit from a first node an ephemeral message encrypted with said ephemeral encryption key; and

means for decrypting said ephemeral message within said tamper resistant cryptographic processor unit using said ephemeral decryption key in the event said message is associated with a message time prior to said expiration time.

42. A method for performing ephemeral decryption comprising:

associating an expiration time with at least an ephemeral decryption key of an ephemeral key pair comprising said ephemeral decryption key and an ephemeral encryption key;

ATTORNEY DOCKET NO. P5529
WEINGARTEN, SCHURGIN,
GAGNEBIN & HAYES LLP
TEL. (617) 542-2290
FAX. (617) 451-0313

storing at least said ephemeral decryption key in a memory within a tamper resistant cryptographic processor unit such that said ephemeral decryption key is not accessible external of said tamper resistant cryptographic processor unit;

comparing a time stamp associated with an encrypted ephemeral message with said expiration time, wherein said encrypted ephemeral message is encrypted with said ephemeral encryption key; and

decrypting said encrypted ephemeral message within said tamper resistant cryptographic processor unit using said ephemeral decryption key if said time stamp is prior to said expiration time.

43. A method for employing ephemeral keys comprising:

associating a time duration defined by an initial value and an ending value with at least an ephemeral decryption key of an ephemeral key pair comprising said ephemeral decryption key and an ephemeral encryption key;

storing at least said ephemeral decryption key in a memory within a tamper resistant cryptographic processor unit such that said ephemeral decryption key is not accessible external of said tamper resistant cryptographic processor unit;

modifying said duration value in a predetermined manner between said initial value and said ending value;

extinguishing at least said ephemeral decryption key within said tamper resistant cryptographic processor unit after said duration value reaches said ending value.

44. The method of claim 43 further including the steps of:

receiving at said tamper resistant cryptographic processor unit an ephemeral message encrypted with said ephemeral encryption key; and

decrypting said ephemeral message within said tamper resistant cryptographic processor unit in the event said duration value has not reached said ending value.

45. The method of claim 43 wherein the difference between said initial value and said ending value corresponds to a time period until expiration of said ephemeral key pair, said ending value equals 0 and said modifying step comprises the step of decrementing said initial value generally periodically until said ending value of 0 is reached.